
PERSONAL DATA PROTECTION IN EDTECH PLATFORMS: LEGAL CHALLENGES AND REGULATORY GAPS

Deeksha Pandey, Research Scholar (PhD in Law, Pursuing), Institute of Legal Studies,
Shri Ram Swaroop Memorial University, Lucknow – Deva Road, Barabanki, 225003

Dr. Purnima Bhardwaj, Assistant Professor, Institute of Legal Studies,
Shri Ram Swaroop Memorial University, Lucknow – Deva Road, Barabanki, 225003

Chapter 1: Introduction

The rapid expansion of digital technology has transformed the education sector in India, giving rise to a dynamic and fast-growing ecosystem of online learning platforms commonly referred to as EdTech (Kumar & Sharma, 2021). This transformation accelerated significantly in the aftermath of the COVID-19 pandemic, when traditional classroom-based education was disrupted and institutions, educators, and students were compelled to shift to virtual modes of learning (UNESCO, 2020). As a result, EdTech platforms emerged not merely as supplementary tools but as central actors in the delivery of education (Jena, 2020). From school-level tutoring applications to advanced professional learning platforms, the EdTech industry in India has witnessed unprecedented growth, attracting large-scale user participation and investment (KPMG, 2021).

While this digital shift has enhanced accessibility, flexibility, and personalization in education, it has simultaneously led to the large-scale collection and processing of personal data (OECD, 2021). EdTech platforms routinely gather a wide range of information from users. This includes basic personal data such as names, contact details, age, and academic records, which are necessary for registration and service delivery (Solove, 2021). However, the scope of data collection extends far beyond these essentials. Many platforms also collect sensitive and behavioral data, including learning patterns, performance analytics, device information, location data, and, in some cases, biometric identifiers such as facial images or voice recordings (ICO, 2020). These data points are often used to develop personalized learning experiences through algorithmic analysis and artificial intelligence-driven tools (Zuboff, 2019).

The increasing reliance on such data-intensive systems raises critical concerns about privacy in the educational context (Nissenbaum, 2010). Education is not merely a commercial service; it is closely linked to individual development, autonomy, and dignity (Sen, 1999). Students,

particularly minors, constitute a vulnerable category of data subjects who may lack the awareness or capacity to fully understand the implications of data sharing (Livingstone et al., 2018). The collection and use of their personal information without adequate safeguards can lead to risks such as profiling, surveillance, unauthorized data sharing, and potential misuse (European Data Protection Board, 2020). Therefore, ensuring privacy within EdTech platforms is not only a matter of regulatory compliance but also a question of protecting fundamental rights and ethical standards in education (Floridi et al., 2018).

In India, the legal landscape governing data protection has undergone a significant shift with the enactment of the Digital Personal Data Protection Act, 2023 (Government of India, 2023). This legislation establishes a general framework for the processing of personal data and outlines obligations for entities classified as data fiduciaries (Bhandari & Bansal, 2023). Although the Act represents a crucial step towards strengthening data protection, it does not specifically address the unique challenges posed by EdTech platforms (Greenleaf, 2023). Issues such as children's data protection, informed consent in digital learning environments, and the use of artificial intelligence for educational profiling remain inadequately regulated (Taylor et al., 2022). Consequently, a gap persists between the rapid technological advancement of EdTech services and the capacity of existing legal frameworks to effectively govern them (De Hert & Papakonstantinou, 2016).

Against this backdrop, the present study seeks to examine the regulatory challenges associated with personal data protection in EdTech platforms. The central research problem lies in the absence of a comprehensive and sector-specific regulatory approach that addresses the distinct risks posed by data-driven educational technologies (Cohen, 2019). While general data protection principles exist, their application to the EdTech context raises complex questions regarding consent, accountability, transparency, and enforcement (Kuner et al., 2020).

The primary objectives of this research are threefold. First, it aims to analyse the nature and extent of personal data collection and processing within EdTech platforms. Second, it seeks to critically evaluate the adequacy of the existing legal framework in addressing privacy concerns in this sector. Third, the study intends to identify regulatory gaps and propose measures to strengthen data protection mechanisms in the context of digital education.

In order to achieve these objectives, the study is guided by several key research questions:

- To what extent do EdTech platforms collect and process personal and sensitive data?
- Are existing data protection laws in India sufficient to regulate such practices?
- What are the specific legal and ethical challenges associated with data protection in EdTech?
- How can regulatory frameworks be improved to ensure effective protection of users, particularly children?

The research adopts a doctrinal and analytical methodology, focusing on the examination of statutory provisions, legal principles, and relevant policy frameworks (IRAC method; Hutchinson, 2018). A comparative approach is also employed to assess how other jurisdictions address similar issues, thereby offering insights for potential reform in India (Van Hoecke, 2011). Additionally, the study incorporates case-based analysis of selected EdTech platforms to understand real-world data practices and identify practical challenges in implementation (Yin, 2018).

In sum, this chapter establishes the foundation for a detailed exploration of personal data protection within the EdTech sector. It highlights the intersection of technology, law, and education, and underscores the urgent need for a more nuanced and effective regulatory approach in an increasingly data-driven learning environment (Westin, 1967).

Chapter 2: Conceptual Framework

A clear conceptual foundation is essential for analysing personal data protection within EdTech platforms (Kuner et al., 2020). The intersection of technology, education, and law involves multiple evolving concepts that must be understood in a structured manner (Floridi et al., 2018). This chapter explains the key terms and principles that form the basis of data protection law, particularly in the Indian context (Bhandari & Bansal, 2023).

Meaning of Personal Data

Personal data refers to any information that relates to an identifiable individual (OECD, 2013). Identification may occur directly, such as through a person's name or identification number, or indirectly, through combinations of data points like location, device identifiers, or academic records (Solove, 2021). In the context of EdTech platforms, personal data typically includes

student names, email addresses, phone numbers, educational history, login credentials, and user-generated content such as assignments or assessments (UNICEF, 2021).

What distinguishes personal data in digital environments is not merely its content but its capacity to be aggregated and analysed (Zuboff, 2019). Even seemingly harmless data points, when combined, can reveal detailed insights about an individual's identity, habits, and preferences (Nissenbaum, 2010). In EdTech ecosystems, such data is continuously generated through user interaction, making its regulation particularly significant (OECD, 2021).

Sensitive Personal Data

Sensitive personal data represents a narrower and more critical category of information that requires a higher degree of protection due to its potential to cause harm if misused (European Data Protection Board, 2020). This includes data relating to health, biometric identifiers, financial information, and other intimate aspects of an individual's life (ICO, 2020). Within EdTech platforms, sensitive data may arise in various forms, such as facial recognition data used for attendance, voice recordings in interactive learning, or behavioural analytics that track cognitive performance and engagement patterns (Taylor et al., 2022).

The sensitivity of such data lies in its potential consequences (Solove, 2021). Unauthorized disclosure or misuse can lead to discrimination, profiling, or psychological harm (Floridi et al., 2018). When minors are involved, the risks are amplified, as they may lack the capacity to understand or consent to such data practices (Livingstone et al., 2018).

Data Fiduciary and EdTech Platforms

The concept of a data fiduciary is central to modern data protection law (Kuner et al., 2020). A data fiduciary is any entity that determines the purpose and means of processing personal data (Government of India, 2023). In the Indian legal framework, particularly under the Digital Personal Data Protection Act, 2023, EdTech platforms fall within this category because they decide how and why user data is collected, stored, and utilised (Bhandari & Bansal, 2023).

The term “fiduciary” implies a relationship of trust (Cohen, 2019). It suggests that the entity handling personal data must act in the best interests of the data subject, similar to how a trustee manages assets on behalf of a beneficiary (Kuner et al., 2020). However, in practice, EdTech companies often operate as commercial enterprises driven by profit motives, which may

conflict with their fiduciary obligations (Zuboff, 2019). This tension raises important legal and ethical questions regarding accountability and responsibility (Floridi et al., 2018).

Privacy as a Fundamental Right

The recognition of privacy as a fundamental right in India marks a significant development in constitutional law (Chandrachud, 2017). In the landmark case of *Justice K.S. Puttaswamy v. Union of India*, the Supreme Court affirmed that the right to privacy is an intrinsic part of the right to life and personal liberty under Article 21 of the Constitution (Supreme Court of India, 2017).

This recognition has far-reaching implications for data protection (Greenleaf, 2023). Privacy is no longer viewed merely as a statutory concern but as a constitutional guarantee that safeguards individual autonomy, dignity, and freedom (Sen, 1999). In the educational context, this becomes particularly relevant, as students must be able to learn and interact in environments that respect their personal space and informational boundaries (UNICEF, 2021). Any intrusion into this space must satisfy the tests of legality, necessity, and proportionality (Supreme Court of India, 2017).

Evolution of Data Protection Law in India

India's journey towards a comprehensive data protection regime has been gradual and multi-layered (Greenleaf, 2023). Initially, data protection was addressed through scattered provisions, such as those found in the Information Technology Act, 2000 and its associated rules (Government of India, 2000). These provisions provided limited safeguards and were largely focused on data security rather than privacy (De Hert & Papakonstantinou, 2016).

The recognition of privacy as a fundamental right created momentum for a more structured legal framework (Chandrachud, 2017). Various expert committees were constituted to draft comprehensive legislation, leading to multiple iterations of data protection bills (Bhandari & Bansal, 2023). This process culminated in the enactment of the Digital Personal Data Protection Act, 2023, which represents India's first dedicated statute on personal data protection (Government of India, 2023).

Despite this progress, the law remains in a developmental phase, with several aspects requiring clarification and refinement, particularly in sector-specific contexts such as education (Taylor

et al., 2022).

Key Principles of Data Protection

Data protection law is guided by certain foundational principles that ensure fairness and accountability in data processing (OECD, 2013). Among these, three principles are especially relevant to EdTech platforms.

Consent

Consent is the cornerstone of lawful data processing (Kuner et al., 2020). It requires that individuals are informed about the nature and purpose of data collection and voluntarily agree to it (ICO, 2020). In theory, consent empowers users to control their personal information (Solove, 2021). However, in practice, especially within EdTech platforms, consent mechanisms are often embedded in lengthy and complex privacy policies that users rarely read or fully understand (Nissenbaum, 2010).

For students, particularly minors, the issue becomes even more complicated (Livingstone et al., 2018). The validity of consent depends not only on its form but also on the capacity of the individual to comprehend its implications (UNICEF, 2021). This raises concerns about whether consent obtained in digital learning environments can truly be considered informed and meaningful (Taylor et al., 2022).

Purpose Limitation

The principle of purpose limitation mandates that personal data should be collected for specific, explicit, and legitimate purposes, and should not be used beyond those purposes without further authorization (OECD, 2013). In the EdTech context, data collected for educational delivery should not be repurposed for unrelated activities such as targeted advertising or commercial profiling without proper safeguards (European Data Protection Board, 2020).

However, the integration of analytics and artificial intelligence often blurs the boundaries of purpose (Zuboff, 2019). Data initially collected for learning improvement may later be used for behavioural prediction or monetisation, raising questions about compliance with this principle (Cohen, 2019).

Data Minimization

Data minimization requires that only the data necessary for a specified purpose should be collected and processed (ICO, 2020). This principle seeks to limit excessive data collection and reduce the risks associated with data breaches or misuse (Solove, 2021).

In practice, many EdTech platforms adopt a data-maximisation approach, collecting extensive information to enhance their services or gain competitive advantages (Zuboff, 2019). This tendency conflicts with the principle of minimization and highlights the need for stricter regulatory oversight (Kuner et al., 2020).

In conclusion, this chapter establishes the conceptual framework necessary for understanding personal data protection in EdTech platforms (Floridi et al., 2018). By clarifying key definitions and principles, it lays the groundwork for a deeper examination of legal provisions, challenges, and regulatory gaps in the chapters that follow (Greenleaf, 2023).

Chapter 3: Legal Framework Governing EdTech Data

The regulation of personal data in India has entered a new phase with the enactment of the Digital Personal Data Protection Act, 2023 (Government of India, 2023). This statute establishes a general framework for processing digital personal data and applies across sectors, including education technology platforms (Bhandari & Bansal, 2023). Although it is not designed specifically for EdTech, its provisions significantly influence how such platforms collect, use, and manage user data (Greenleaf, 2023).

At its core, the Act recognises the relationship between the individual (data principal) and the entity processing data (data fiduciary) (Kuner et al., 2020). EdTech platforms qualify as data fiduciaries because they determine the purpose and means of processing student data (Government of India, 2023). Consequently, they are bound by statutory obligations that aim to ensure lawful and fair data handling (De Hert & Papakonstantinou, 2016).

A central institutional feature of the Act is the Data Protection Board of India (Government of India, 2023). This body is responsible for overseeing compliance, adjudicating disputes, and imposing penalties in cases of violation (Bhandari & Bansal, 2023). While the Board represents a step toward institutional accountability, questions remain regarding its independence, capacity, and effectiveness in handling complex, technology-driven disputes involving EdTech

platforms (Greenleaf, 2023).

The applicability of the Act to EdTech platforms is broad (Government of India, 2023). Any platform that processes digital personal data within India, or offers services to Indian users, falls within its scope (Kuner et al., 2020). This includes learning applications, virtual classrooms, and AI-driven educational tools (OECD, 2021). However, the absence of sector-specific rules means that general provisions must be interpreted in the context of education, which can lead to ambiguity (Taylor et al., 2022).

Data fiduciaries under the Act are subject to several obligations (Government of India, 2023). They must ensure that data is processed for lawful purposes, maintain accuracy, implement reasonable security safeguards, and prevent unauthorized access or breaches (ICO, 2020). They are also required to provide clear notices regarding data usage and to delete data once the purpose of collection is fulfilled (Kuner et al., 2020). In the EdTech context, this implies that platforms should not retain student data indefinitely or use it beyond educational objectives without justification (OECD, 2021).

The Act also recognises certain rights of data principals, which in the EdTech setting primarily include students and, in the case of minors, their guardians (Government of India, 2023). The right to access enables users to obtain information about the data collected and how it is being used (Solove, 2021). The right to correction allows them to rectify inaccurate or outdated information, which is particularly important for academic records (ICO, 2020). Additionally, the right to grievance redressal provides a mechanism through which users can raise concerns regarding misuse or mishandling of their data (Bhandari & Bansal, 2023). While these rights are significant, their practical effectiveness depends on awareness, accessibility, and enforcement (Greenleaf, 2023).

Overall, the legal framework establishes a foundational structure for data protection in EdTech (De Hert & Papakonstantinou, 2016). However, its general nature necessitates further interpretation and refinement to address the specific realities of digital education (Taylor et al., 2022).

Chapter 4: Data Practices in EdTech Platforms

EdTech platforms operate through diverse models, each involving distinct forms of data

collection and processing (OECD, 2021). Broadly, these platforms can be categorised into three types: learning applications, live class platforms, and AI-based learning systems (KPMG, 2021).

Learning applications typically provide pre-recorded content, quizzes, and self-paced modules (Jena, 2020). These platforms collect user registration details along with data on course preferences, progress, and performance (UNICEF, 2021). Live class platforms, on the other hand, facilitate real-time interaction between teachers and students, often involving video, audio, and chat-based communication (OECD, 2021). Such platforms collect not only personal identifiers but also recordings of sessions and participation metrics (ICO, 2020).

AI-based learning systems represent a more advanced category, relying on algorithms to personalise education (Zuboff, 2019). These platforms analyse user behaviour, learning speed, and response patterns to tailor content (Taylor et al., 2022). While this enhances efficiency, it also increases the volume and sensitivity of data processed (Floridi et al., 2018).

A defining feature of EdTech platforms is their reliance on continuous data collection (OECD, 2021). Student behaviour is tracked through clicks, time spent on tasks, and engagement levels (Nissenbaum, 2010). Performance analytics are generated to assess strengths and weaknesses, often forming the basis for personalised recommendations (Solove, 2021). While these practices improve learning outcomes, they also create detailed digital profiles of users (Zuboff, 2019).

Artificial intelligence plays a crucial role in this ecosystem (Floridi et al., 2018). Algorithms process large datasets to predict performance, suggest courses, and even identify potential learning difficulties (Taylor et al., 2022). However, such profiling can lead to unintended consequences, including stereotyping or limiting opportunities based on past performance (Cohen, 2019).

Another important aspect is the monetisation of data (Zuboff, 2019). Although many platforms claim to prioritise education, data is often used for commercial purposes such as targeted advertising, partnerships, or product development (OECD, 2021). This raises concerns about whether educational data is being treated as a commodity rather than a protected resource (Cohen, 2019).

Case-based analysis reveals that many platforms lack transparency in their data practices (ICO, 2020). Privacy policies are often complex, and users may not fully understand how their data is being utilised (Nissenbaum, 2010). This gap between formal compliance and actual practice highlights the need for closer scrutiny (Kuner et al., 2020).

Chapter 5: Legal Challenges in EdTech Data Protection

Despite the existence of a statutory framework, several legal challenges complicate the protection of personal data in EdTech platforms (Greenleaf, 2023). One of the most prominent issues is the lack of informed consent (Kuner et al., 2020). Privacy policies are frequently lengthy and technical, making it difficult for users to comprehend the scope of data collection and processing (Nissenbaum, 2010). As a result, consent is often obtained in a formal sense but lacks substantive understanding (Solove, 2021).

The protection of minors' data presents an additional layer of complexity (Livingstone et al., 2018). A significant proportion of EdTech users are children, yet mechanisms for age verification remain inadequate (UNICEF, 2021). Platforms may rely on self-declaration, which is unreliable and does not ensure meaningful parental involvement (Taylor et al., 2022). This raises concerns about the validity of consent and the adequacy of safeguards (ICO, 2020).

Excessive data collection is another challenge (OECD, 2021). Many platforms gather more information than is necessary for educational purposes, driven by the desire to enhance analytics or generate revenue (Zuboff, 2019). This practice conflicts with the principle of data minimization and increases the risk of misuse (Kuner et al., 2020).

Algorithmic profiling further complicates the legal landscape (Floridi et al., 2018). AI systems may introduce bias or reinforce existing inequalities, particularly when trained on incomplete or skewed datasets (Cohen, 2019). The absence of clear legal standards for algorithmic accountability makes it difficult to address such issues (Taylor et al., 2022).

Data breaches and weak cybersecurity measures also pose significant risks (ICO, 2020). Educational platforms may not always invest in robust security infrastructure, leaving sensitive student data vulnerable to unauthorized access (OECD, 2021). The consequences of such breaches can be severe, especially when they involve minors (UNICEF, 2021).

Finally, cross-border data transfers create jurisdictional challenges (Greenleaf, 2023). Many

EdTech platforms operate globally, storing and processing data in multiple locations (Kuner et al., 2020). This complicates enforcement and raises questions about the adequacy of protections in foreign jurisdictions (De Hert & Papakonstantinou, 2016).

Chapter 6: Regulatory Gaps and Weaknesses

While the Digital Personal Data Protection Act, 2023 provides a general framework, several gaps limit its effectiveness in the EdTech sector (Government of India, 2023). One significant limitation is the presence of broad government exemptions, which may allow state authorities to bypass certain safeguards (Bhandari & Bansal, 2023). This raises concerns about the balance between regulatory power and individual privacy (Greenleaf, 2023).

Another major gap is the absence of AI-specific provisions (Taylor et al., 2022). As EdTech increasingly relies on algorithmic systems, the lack of regulation in this area creates uncertainty and potential risks (Floridi et al., 2018). Issues such as transparency, accountability, and fairness in automated decision-making remain largely unaddressed (Cohen, 2019).

The enforcement structure also faces challenges (Government of India, 2023). While the Data Protection Board is tasked with oversight, its capacity to handle large volumes of complaints and complex technological issues is yet to be tested (Bhandari & Bansal, 2023). Without strong enforcement, legal provisions may remain ineffective in practice (Greenleaf, 2023).

The absence of sector-specific regulation for EdTech further exacerbates these issues (OECD, 2021). Education involves unique considerations, particularly when it comes to children's data (UNICEF, 2021). The current framework does not provide detailed guidance tailored to this sector (Taylor et al., 2022).

There is also a lack of clarity regarding children's data protection and the responsibilities of EdTech platforms (Livingstone et al., 2018). This ambiguity makes it difficult to establish accountability and enforce standards (Kuner et al., 2020). Additionally, grievance redressal mechanisms may not be easily accessible or user-friendly, limiting their practical utility (ICO, 2020).

Chapter 7: Comparative Analysis

A comparative perspective helps to identify strengths and weaknesses in India's approach to

data protection (De Hert & Papakonstantinou, 2016). The General Data Protection Regulation (GDPR) is often regarded as a global benchmark due to its comprehensive and stringent provisions (European Data Protection Board, 2020).

One of the key features of the GDPR is its robust consent framework, which emphasises clarity, specificity, and user control (Kuner et al., 2020). Unlike many existing practices in India, consent under the GDPR must be explicit and easily withdrawable (ICO, 2020). This enhances user autonomy and accountability (Solove, 2021).

The GDPR also includes specific provisions for children's data, particularly under Article 8, which requires parental consent for processing data of minors below a certain age (European Data Protection Board, 2020). This reflects a more protective approach compared to the Indian framework (Greenleaf, 2023).

In the United States, the Children's Online Privacy Protection Act (COPPA) provides another model, focusing specifically on the protection of children's online data (FTC, 2019). It imposes obligations on operators of websites and services directed at children, including requirements for parental consent and data security (FTC, 2019).

These international frameworks offer valuable lessons for India (De Hert & Papakonstantinou, 2016). They demonstrate the importance of sector-specific regulation, strong enforcement mechanisms, and clear standards for consent and accountability (Kuner et al., 2020).

Chapter 8: Recommendations and Reform Suggestions

In light of the challenges and gaps identified, several reforms are necessary to strengthen data protection in EdTech platforms (Greenleaf, 2023). First, there is a need for sector-specific guidelines that address the unique characteristics of digital education (OECD, 2021). Such guidelines should provide clarity on permissible data practices and establish minimum standards for compliance (Kuner et al., 2020).

The protection of children's data should be prioritised through stricter requirements for age verification and parental consent (UNICEF, 2021). Platforms should adopt child-friendly privacy policies that are simple and accessible (Livingstone et al., 2018).

Mandatory data audits can enhance accountability by ensuring that platforms regularly assess

their data practices and identify potential risks (ICO, 2020). Similarly, algorithmic transparency should be promoted to address concerns related to bias and profiling (Floridi et al., 2018).

Consent mechanisms should be simplified to ensure that users can make informed decisions without being overwhelmed by technical language (Nissenbaum, 2010). This may involve the use of layered notices or visual tools (Kuner et al., 2020).

Stronger penalties for violations can act as a deterrent, while independent regulatory oversight can improve enforcement (Government of India, 2023). Together, these measures can create a more balanced and effective framework (Greenleaf, 2023).

Chapter 9: Conclusion

The analysis of personal data protection in EdTech platforms reveals a complex interplay between technological innovation and legal regulation (Floridi et al., 2018). While digital education offers significant benefits in terms of accessibility and efficiency, it also introduces new risks related to privacy and data security (OECD, 2021).

The existing legal framework, centred on the Digital Personal Data Protection Act, 2023, provides a necessary foundation but is not sufficient to address the specific challenges of the EdTech sector (Government of India, 2023). Issues such as children's data protection, algorithmic accountability, and enforcement gaps require targeted attention (Taylor et al., 2022).

There is an urgent need for reforms that align legal standards with technological realities (Greenleaf, 2023). A balanced approach is essential—one that supports innovation while safeguarding the rights and interests of users (Cohen, 2019). By strengthening regulatory mechanisms and promoting responsible data practices, it is possible to create a digital education ecosystem that is both effective and ethically sound (Kuner et al., 2020).

REFERENCES

- Bhandari, V., & Bansal, A. (2023). *Data protection law in India: Analysis of the Digital Personal Data Protection Act, 2023*. Journal of Indian Law and Society, 14(2), 45–67.
- Chandrachud, D. Y. (2017). *Privacy as a fundamental right: Interpretation in Puttaswamy judgment*. Supreme Court Observer.
- Cohen, J. E. (2019). *Between truth and power: The legal constructions of informational capitalism*. Oxford University Press.
- De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review*, 32(2), 179–194.
- European Data Protection Board. (2020). *Guidelines on consent under Regulation 2016/679*.
- Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4People—An ethical framework for a good AI society. *Minds and Machines*, 28(4), 689–707.
- Federal Trade Commission. (2019). *Children's Online Privacy Protection Rule (COPPA)*.
- Government of India. (2000). *Information Technology Act, 2000*.
- Government of India. (2023). *Digital Personal Data Protection Act, 2023*.
- Greenleaf, G. (2023). *Global data privacy laws 2023: India's evolving framework*. Privacy Laws & Business International Report.
- ICO (Information Commissioner's Office). (2020). *Children's code: Age appropriate design code*.
- Jena, P. K. (2020). Impact of COVID-19 on higher education in India. *International Journal of Advanced Education and Research*, 5(3), 77–81.
- KPMG. (2021). *Online education in India: 2021 report*. KPMG India.
- Kuner, C., Bygrave, L. A., & Docksey, C. (2020). *The EU General Data Protection Regulation (GDPR): A commentary*. Oxford University Press.
- Kumar, A., & Sharma, R. (2021). Growth of EdTech sector in India: Opportunities and challenges. *Journal of Educational Technology Systems*, 50(2), 140–158.

Livingstone, S., Stoilova, M., & Nandagiri, R. (2018). Children's data and privacy online: Growing up in a digital age. *London School of Economics Report*.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

OECD. (2013). *OECD guidelines on the protection of privacy and transborder flows of personal data*.

OECD. (2021). *Digital education outlook 2021: Pushing the frontiers with AI, blockchain and robots*.

Sen, A. (1999). *Development as freedom*. Oxford University Press.

Solove, D. J. (2021). *Understanding privacy*. Harvard University Press.

Supreme Court of India. (2017). *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

Taylor, L., Floridi, L., & Van der Sloot, B. (2022). *Group privacy: New challenges of data technologies*. Springer.

UNESCO. (2020). *Education in a post-COVID world: Nine ideas for public action*.

UNICEF. (2021). *Policy guidance on AI for children*.

Westin, A. F. (1967). *Privacy and freedom*. Atheneum.

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Sage Publications.

Van Hoecke, M. (2011). *Methodologies of legal research: What kind of method for what kind of discipline?* Hart Publishing.